Ein sicheres Netzwerk ist möglich

Von Dr. Gerhard Eschelbeck

Für ein sicheres Netzwerk muss man heute etwas tun. Denn Einbruchsversuche werden dadurch begünstigt, dass die Netzwerkgrenzen – aufgrund zahlreicher neuer Zugangspunkte wie Funknetze und Virtual Private Networks – immer durchlässiger werden. Außerdem sind Netzwerke und Anwendungen heute komplexer, wodurch eine Vielzahl angreifbarer Schwachstellen entsteht.

Bei den ersten Virentypen des Internet-Zeitalters war es noch erforderlich, dass die Empfänger verseuchter E-Mails oder die Anwender von Programmen zweifelhafter Herkunft aktiv zur Reproduktion und Verbreitung der Viren beitragen. Dafür reichte oft schon, den Anhang einer E-Mail zu öffnen. Heute sind es selbständig aktive Würmer, die Systeme und Anwendungen angreifen. Sie dringen ein, indem sie Sicherheitslücken in den Systemen und Applikationen ausnutzen; Anwenderaktionen sind dazu nicht erforderlich.



Dr. Gerhard Eschelbeck ist Chief Technical Officer und VP Engineering von Qualys Inc. Er veröffentlichte mit den bekannten „Laws of Vulnerabilities" die erste wissenschaftliche Abhandlung zum Thema „kritische Schwachstellen in Netzwerken" mit Ergebnissen von Millionen von Netzwerkscans. Er wurde bereits mehrfach zu einem der einflussreichsten CTOs der Welt gewählt. Er lehrt „Netzwerk Security" an der Universität Linz und hält zahlreiche Patente im Bereich Managed Network Security.

Künftige Bedrohungen

Die Bedrohungen der nächsten Generation unterscheiden sich von den früheren sowohl durch das Verbreitungstempo als auch durch die Strategien, mit denen Viren, Würmer & Co. ihre Opfer auswählen. Das Ziel besteht darin, in der ersten Stunde in so viele Systeme wie nur möglich einzubrechen, weil dadurch ein Gegenschlag praktisch ausgeschlossen wird. Hier helfen nur regelmäßige Sicherheitsaudits und Schwachstellenanalysen. Sie sind eine effektive Methode, um aktiven Schutz zu installieren, bevor Sicherheitslücken von schädlichen Programmen ausgenutzt werden können.

Analyse der Sicherheitsbedrohungen

Jüngste Sicherheitsattacken weisen erste Merkmale von Angriffsprogrammen der neuesten Generation auf – und demonstrieren eindringlich, welch verheerende Auswirkungen künftige Angriffe haben können. Die Programme haben hinterlistige Eigenschaften. Zunächst einmal verbreiten sie sich rasend schnell. Das ist aus Hackersicht wünschenswert – es verhindert ein rechtzeitiges Eingreifen der Sicherheitsadministratoren und richtet deshalb größere Schäden an. Bei praktisch allen Angriffen in der Vergangenheit wurden allerdings bekannte Sicherheitslücken ausgenutzt. Ein wesentlicher Grund hierfür liegt darin, dass die Entdeckung neuer Schwachstellen harte Arbeit ist und die technischen Fähigkeiten des durchschnittlichen Angreifers übersteigt. Schließlich werden die Angriffe in Zukunft an mehreren Stellen gleichzeitig erfolgen. Besonders anfällig werden viele neue Technologien sein, weil sie mit keinen weit reichenden Funktionen zur Erkennung von Bedrohungen und zum Schutz vor ihnen ausgestattet sind. Doch es gibt wirksame Abwehrstrategien.

Sicherheit durch ständige Überwachung

Regelmäßige Sicherheitsaudits, bei denen Schwachstellen in Systemen und Anwendungen analysiert werden, sind ein wichtiges Mittel, um eine starke Abwehr zu gewährleisten. Die Methoden reichen von herkömmlichen Durchdringungstests bis zu neuen, automatisierten Diensten, die über das Web durchgeführt werden. Zu einem gründlichen Audit gehört, die Antiviren-Software auf dem neuesten Stand zu halten, Programme und Betriebssysteme regelmäßig aufeinander abzustimmen und die Sicherheitsrichtlinien des Unternehmens laufend zu überprüfen – das heißt, sie mit der Praxis im Arbeitsalltag abzugleichen.

Fassen wir zusammen: Die Angriffe auf die Netzwerksicherheit werden immer zahlreicher und raffinierter. Hacker nützen die Erfahrungen, um eine neue Generation automatisierter Bedrohungen zu entwickeln. Die Angriffe der Zukunft werden sich schneller ausbreiten, als jede menschenmögliche Gegenwehr greifen kann. Die rechtzeitige und umfassende Erkennung von Sicherheitslücken und die rasche Durchführung von Abhilfemaßnahmen sind die wirkungsvollsten Vorkehrungen, die die Sicherheitsadministratoren treffen können, um automatisierte Angriffe abzuwehren und die Sicherheit ihrer Netzwerke zu wahren.